1 **INSERTING AND DETECTING WATERMARKS IN IMAGES DERIVED FROM A**

2 **SOURCE IMAGE**

3 **FIELD OF THE INVENTION**

4 This application is directed to the field of digital imaging. It
5 is more specifically concerned with the insertion of identifying
6 marks in a source digital image, and the detection of those same
7 identifying marks in a set of images of different sizes that are
8 derived from the source digital image.

9 **BACKGROUND OF THE INVENTION**

10 Various invisible watermarking techniques are known to those
11 skilled in the art. Each technique generally has different
12 advantages and satisfies different levels of robustness, security
13 and adaptability. Many of these employ particular algorithms in
14 determining how the pixel data of pixels in the unmarked source
15 digital image is to be modified in order to include the
16 particular watermark. In general, each watermark inserting
17 technique has a corresponding watermark detecting technique. The
18 common feature of most of these techniques is that the pixel
19 data, or the resulting pel data, is ultimately modified in a
20 particular way that is intended to make the modification unseen.

21 It is a constant endeavor to find improved techniques of placing
22 invisible identifying marks, herein called watermarks, into a
23 digital image. The ability to detect the presence of watermarks
24 in a digital image is generally useful to help establish

1 ownership, origin and authenticity, and also to discourage those
2 who might wish to misappropriate the work. Identifying marks are
3 also useful to give evidence of unauthorized disclosure.
4 Heretofore watermarking methods have been concerned with
5 inserting a watermark into a *digital image* after it is enlarged
6 or reduced in size, herein called *resizing*, for presentation. For
7 an inserted watermark to be subsequently detected, many image
8 watermarking methods require that every copy of a watermarked
9 digital image must be restored to its presentation size so a
10 one-to-one pixel position correlation with elements in a
11 watermarking plane can be achieved before detection is attempted.
12 If a derived image is not resized correctly and its pixel's
13 positions are not correlated one-to-one with elements of its
14 appropriate watermarking plane, watermark detection will fail.

15 **SUMMARY OF THE INVENTION**

16 Thus, the present invention provides a watermarking technique
17 whereby a watermark is inserted into a digital image that is
18 bounded by a specific *bounding rectangle*. If the source image is
19 larger horizontally and/or vertically than the bounding
20 rectangle, it is reduced in the horizontal dimension by a
21 horizontal factor and in the vertical dimension by a vertical
22 factor until it lies totally within the bounding rectangle with
23 at least one pair of its parallel edges touching parallel edges
24 of the bounding rectangle. If the source image is smaller
25 horizontally and vertically than the bounding rectangle, it is
26 enlarged by a horizontal factor and vertical factor in horizontal
27 and vertical dimension until at least one pair of its parallel
28 edges touch parallel edges of the bounding rectangle.

29 In an advantageous embodiment the horizontal factor and vertical

1 factors are equal. If they differ at all, the difference must be
2 small to avoid distorting the appearance of the image. Thus, if
3 the source image is larger horizontally and/or vertically than
4 the bounding rectangle, it is reduced in both horizontal and
5 vertical dimensions by a common factor until it lies totally
6 within the bounding rectangle with at least one pair of its
7 parallel edges touching parallel edges of the bounding rectangle.
8 If the source image is smaller horizontally and vertically than
9 the bounding rectangle, it is enlarged by a common factor in
10 horizontal and vertical dimension until at least one pair of its
11 parallel edges touch parallel edges of the bounding rectangle.
12 (Regardless of the shape of the source image, the resized image
13 is the largest image that will fit entirely within the bounding
14 rectangle.) The reduced or enlarged image, or the source image if
15 resizing is not needed, is called an *adjusted image*. Then,
16 regardless of the size of an image derived from the watermarked
17 adjusted image, enlarging or reducing the derived image to touch
18 at least one pair of parallel edges of the specific bounding
19 rectangle, and with the resized image contained entirely within
20 the bounding rectangle, greatly facilitates detection of the
21 imbedded watermark.

22 It is an aspect of the present invention to provide methods,
23 systems and apparatus for resizing a source image so that the
24 resized image lies entirely within a specified bounding
25 rectangle, with at least one pair of its parallel edged touching
26 parallel edges of the bounding rectangle.

27 Another aspect of the present invention provides methods, systems
28 and apparatus for inserting an invisible watermark into the
29 adjusted image. After watermark insertion into an adjusted image,
30 the present invention includes forming at least one derived image
31 by further resizing of the watermarked adjusted image.

1 In another aspect of the present invention, the size of the
2 bounding rectangle chosen may be specific to each source image,
3 or, conversely, a common bounding rectangle may be used for a
4 group of source images.

BRIEF DESCRIPTION OF THE DRAWINGS

6 These and other aspects, features, and advantages of the present
7 invention will become apparent upon further consideration of the
8 following detailed description of the invention when read in
9 conjunction with the drawing figures, in which:

10 Fig. 1 shows an example of a watermarking insertion procedure in
11 accordance with the present invention;

12 Fig. 2 shows an example of a watermarking detection procedure in
13 accordance with the present invention; and

14 Fig. 3 shows an example of an alternative method for producing
15 watermarked derivative images.

DETAILED DESCRIPTION OF THE INVENTION

17 The present invention provides methods, systems and apparatus for
18 a watermarking technique whereby a watermark is inserted into a
19 digital image that is bounded by a specific *bounding rectangle*.
20 The bounding rectangle has dimensions of M pixels wide and N
21 pixels high. If the source image is larger horizontally and/or
22 vertically than the bounding rectangle, it is reduced in both
23 horizontal and vertical dimensions by horizontal and vertical

1 factors, or by a common factor, until it lies totally within the
2 bounding rectangle with at least one pair of its parallel edges
3 touching parallel edges of the bounding rectangle. If the source
4 image is smaller horizontally and vertically than the bounding
5 rectangle, it is enlarged by a common factor in horizontal and
6 vertical dimension until at least one pair of its parallel edges
7 touch parallel edges of the bounding rectangle. The reduced or
8 enlarged image, or the source image if resizing is not needed, is
9 called an *adjusted image.* Then, regardless of the size of an
10 image derived from the watermarked adjusted image, enlarging or
11 reducing the derived image to touch at least one pair of parallel
12 edges of the specific bounding rectangle, and with the resized
13 image contained entirely within the bounding rectangle,
14 facilitates detection of the imbedded watermark.

15 In a particular embodiment, the present invention provides
16 methods, systems and apparatus for resizing a source image so the
17 resized image lies entirely within a specified bounding rectangle
18 with at least one pair of its parallel edged touching parallel
19 edges of the bounding rectangle. The image so produced is called
20 an adjusted image. There are many methods for resizing digital
21 images known to those skilled in the art. Nearly any one of them
22 may be used for resizing purposes providing the chosen method
23 preserves the ratio of image width to image height.

24 The present invention employs methods for inserting an invisible
25 watermark into the adjusted image. After watermark insertion into
26 an adjusted image, the present invention provides methods,
27 systems and apparatus for forming at least one derived image by
28 further resizing of the watermarked adjusted image.

29 In a general embodiment, the size of the bounding rectangle
30 chosen may be specific to each source image, or, conversely, a

1 common bounding rectangle may be used for a group of source

2 images. Generally, there is limitation of the useful range of the

3 resizing factor, which relates the dimensions of the smallest

4 desired derivative image and the dimensions of the bounding

5 rectangle. A value of the resizing factor that is less than 0.1

6 makes the probability of detecting the imbedded watermark small.

7 However, since detection is a probabilistic event dependent on

8 the watermarking method chosen and on the image being

9 watermarked, for some cases this factor can be still smaller. A

10 usually useful resizing factor is greater than 0.125, for the

11 watermarking method in the example embodiment.

12 The present invention is adaptable for use with any of many

13 watermarking techniques. It is most particularly adaptable to a

14 watermarking technique employing a watermarking plane. Thus,

15 although the present invention is adaptable to many watermarking

16 techniques, it is most easily described and adaptable to the

17 watermark inserting and detecting methods described in US Patent

18 5,530,759 and US Patent 5,825,892 which are herein included by

19 reference in entirety for all purposes.

20 There are advantages to inserting a watermark into a digital

21 image, or a set of digital images, at a common size before it is

22 resized to its presentation size. In this case, any candidate

23 watermarked image can be restored to the common size and a

24 detection may be attempted on that restored-size image. If the

25 converse is true, the candidate image must be restored to each of

26 the presentation sizes prepared from its source image and

27 detection must be attempted at each of the presentation sizes. If

28 the system produces n presentation-sized versions of the source

29 image, on average half that number, $n/2$, detections would be

30 required. If the system produces presentation images at a very

31 large number of resolutions, as would be done with a

1 "continuously-variable" zoom, the number of detections required
2 for a candidate image would be very large.

3 Invisible marks are herein classified relative to the appearance
4 of that mark to a human being with normal visual acuity. A mark
5 inserted into an image is classified as having an invisibility
6 classification level of *undetectably invisible* if, when the image
7 without the marking is displayed together with an image copy with
8 the marking, the human being is equally likely to select either
9 of these copies as an unmarked copy. An undetectably invisible
10 mark is below or at the human being's threshold of
11 just-noticeable difference. A mark on an image is classified as
12 having an invisibility classification level of *subliminally*
13 *invisible* if the mark is not distracting to the human being,
14 although it is above the human being's threshold of
15 just-noticeable difference. An image marking is classified as
16 being *marginally invisible* if it does not cause the marked image
17 to lose its usefulness or value because of the mark. An image
18 marking is classified as being *poorly invisible* if the marking is
19 relatively obvious or distracting, and causes a reduction in the
20 image's usefulness and/or value.

21 Presently, invisible markings of digital images are used as a
22 generally dependable method of establishing evidence of ownership
23 and authenticity. A digital image is an abstraction of a physical
24 image that has been scanned or artificially created and stored in
25 a computer's memory as rectangular arrays of numbers
26 corresponding to that image's (one or more) color planes. Each
27 array element corresponds to a very small area of the physical
28 image and is called a picture element, or *pixel*. The numeric
29 value associated with each pixel for a monochrome image
30 represents the magnitude of its average brightness of its single
31 color (for example, black and white) plane. For a color image,

1 each pixel of the digital image has values associated and
2 representing the magnitudes of average brightness of its color
3 components represented in its three or more color planes.

4 Whenever reference is made herein to color planes, it is
5 understood to include any number of color planes used by a
6 particular image's digitizing technique to define the pixel's
7 color characteristics. This includes the case when there is only
8 a single plane defining a monochromatic image. Pixel values have
9 a magnitude represented by at least one binary digit or bit.

10 Generally, a digital image is recognizable as an image to a
11 viewer only when the individual pixels are displayed as dots of
12 white or colored light on a display, or as dots of black or
13 colored inks on paper. Pixels are normally spaced so closely as
14 to be not resolvable by a human visual system. This results in
15 the fusion of neighboring pixels by the human visual system into
16 a representation of the original physical image. Image fusion by
17 the human visual system makes invisible marking, or relatively
18 invisible marking, of images possible. This property is fully
19 exploited by the methods described here to both insert an
20 invisible watermark into a digital image or digital image to a
21 desired invisibility classification, and to subsequently
22 demonstrate its existence. The inserting and demonstrated
23 detection of a robust invisible marking on digital and printed
24 digital images called hard copy images, herein called invisible
25 watermarking, are primary aspects of the present invention.

26 A proper invisible watermarking technique that inserts an
27 invisible watermark into a digital image should satisfy several
28 properties. The inserted watermark should appear to be invisible
29 to any person having normal or corrected to normal visual
30 accommodation to a desired invisibility classification level.

1 Clearly, the degree of marking is a dichotomy. A balance has to

2 be struck between protecting the image from unauthorized uses and

3 not having the watermark unpleasantly alter the appearance of the

4 image. This generally means that a recognizable pattern should

5 not be apparent in the marked image when the watermark is applied

6 to a uniformly colored plane. This requirement discourages

7 marking the image by varying the hue of its pixels, since the

8 human visual system is significantly more sensitive to

9 alterations in hue than in brightness. The requirement can be

10 satisfied by a technique based on varying picture element

11 brightness implemented in a proper way. A technique based on

12 varying picture element brightness also allows the same marking

13 technique applied to color images to be equally applicable to

14 monochrome images.

15 Another property of a proper invisible watermarking technique is

16 that it should have a detection scheme such that the probability

17 of a false-positive detection, that is, the false detection of a

18 mark when one, in fact, does not exist, is very small. For

19 purposes of the present invention, the probability of detection

20 of a watermark in an image when one does not exist should be less

21 than one in a million. There is generally little difficulty

22 satisfying this requirement when the technique is statistically

23 based.

24 Still another property of a proper watermarking technique is that

25 it should be possible to vary the degree of marking applied to an

26 image. In this way, the watermark can be made as detectable as

27 necessary by the particular application. This property is

28 important in highly textured images where it is often necessary

29 to increase the intensity of the mark to increase its likelihood

30 of detection. This is in contradistinction with images that have

31 low contrast in which it is advantageous to reduce the marking

1 intensity to lessen undesirable visible artifacts of the
2 watermark itself.

3 Finally, the inserted watermark should be robust in that it
4 should be very difficult to be removed or rendered undetectable.
5 It should survive such image manipulations that in themselves do
6 not damage the image beyond usability. This includes, but is not
7 limited to, JPEG "lossy" compression, image rotation, linear or
8 nonlinear resizing, brightening, sharpening, "despeckling," pixel
9 editing, color-space conversion, the malicious superposition of a
10 correlated or uncorrelated noise field upon the digital image,
11 and its subsequent conversion to halftone and printing. Attempts
12 to defeat or remove the watermark should be generally more
13 laborious and costly than purchasing rights to use the image. If
14 the image is of rare value, it is desirable that the watermark be
15 so difficult to remove that telltale traces of it can almost
16 always be recovered.

17 It will be clear to those skilled in the art that other
18 modifications to the disclosed embodiments can be effected
19 without departing from the spirit and scope of the invention. The
20 embodiments described below, ought to be construed to be merely
21 illustrative of some of the more prominent features and
22 applications of the invention. Other beneficial results can be
23 realized by applying the disclosed invention in a different
24 manner or modifying the invention in ways known to those familiar
25 with the art.

26 Referring to Figure 1, the watermarking procedure described so
27 far may be viewed as first providing a monochrome or color
28 digital source image (101), specifying the dimensions of a
29 desired bounding rectangle (103) into which the source image will
30 be enlarged or reduced to fit. If the source image is larger

1 horizontally and/or vertically than the bounding rectangle, it is
2 reduced in both horizontal and vertical dimensions by a common
3 first factor **f1**, which is less than 1, until it lies totally
4 within the bounding rectangle with at least one pair of its
5 parallel edges touching parallel edges of the bounding rectangle.
6 If the source image is smaller horizontally and vertically than
7 the bounding rectangle, it is enlarged in horizontal and vertical
8 dimension by the common factor **f1**, which is greater than 1, until
9 at least one pair of its parallel edges touch parallel edges of
10 the bounding rectangle (105). The reduced or enlarged source
11 image, or the source image itself if resizing is not needed, is
12 called an *adjusted image*. An invisible watermark is then imbedded
13 into that adjusted image (107). Finally, the watermarked adjusted
14 image is resized by a second factor, **f2.** There can be as many
15 different values of **f2** as desired, with each different value
16 producing a differently sized derivative image (109).

17 Detecting the watermark in a candidate image, regardless of the
18 size of the candidate image, becomes a common procedure.
19 Referring to Figure 2, the dimensions of the bounding rectangle
20 used produce the resized source image to which the candidate
21 image corresponds are recalled (201). The candidate image is
22 resized, if necessary, to form a resized candidate image that is
23 as large as will fit into the recalled bounding rectangle, having
24 at least one pair of the resized candidate image's parallel edges
25 touching a pair of parallel edges of the recalled bounding
26 rectangle (203). The watermark suspected of being imbedded in the
27 candidate image is recalled or reproduced (205), and an attempt
28 is made to detect the recalled or reproduced watermark in the
29 resized candidate image (207).

30 One skilled in the art will recognize that, alternatively, the
31 reduction steps in the process may be rearranged to produce an

1 equivalent watermarked image of the same size. Referring to
2 Figure 3, those rearranged steps require first providing a
3 monochrome or color digital source image (301), specifying the
4 dimensions of a desired bounding rectangle (303), determining the
5 resizing factor **f1** that, if it were to be applied, would resize
6 the source image to fit into the bounding rectangle (305);
7 resizing the source image by the combined factor **f1** times **f2** to
8 form an alternative adjusted image (307); resizing the
9 watermarking plane by the factor **f2** to form an adjusted watermark
10 (309); and lastly, inserting the adjusted watermark into the
11 alternative adjusted image to form a prototype watermarked image
12 (311). As many individual derivative images of different sizes
13 may then be made by resizing the prototype watermarked image
14 (313).

15 Thus the present invention includes a method including the steps
16 of: obtaining a digitized image to be protected by a watermark;
17 specifying a digitized bounding rectangle having known horizontal
18 and vertical dimensions; forming a resized image by resizing the
19 horizontal and vertical dimensions of the image by a horizontal
20 factor and a vertical factor, or a common factor, so that the
21 resized image is a largest replica of the digitized image fitting
22 entirely within the bounding rectangle; and imbedding the
23 watermark into the resized image to form a watermarked image.

24 In some embodiments the common factor is greater than 0.1. In
25 some embodiments, the method includes forming at least one
26 derivative copy of the watermarked image. Each copy preserves the
27 ratio of horizontal dimension to vertical dimension an nearly as
28 practicable.

29 The present invention also includes a method for inserting a
30 watermark into at least one derivative image, including the steps

1 of: providing a source digital image having at least one image

2 plane, each image plane being represented by an array having

3 pixel brightness data for a plurality of pixels, each of the

4 pixels having at least one color component and having a pixel

5 position; specifying horizontal and vertical dimensions of a

6 bounding rectangle; resizing the source image by enlargement or

7 reduction of its horizontal and vertical dimensions by a common

8 factor to form an adjusted image so that the resized image is a

9 largest replica of the digitized image fitting entirely within

10 the bounding rectangle; inserting into the adjusted digital image

11 an invisible image watermark; and producing at least one derived

12 image by resizing the watermarked adjusted image.

13 The present invention also includes a method for inserting a

14 watermark into at least one derived image, including the steps

15 of: providing a source digital image having at least one image

16 plane, each image plane being represented by an array having

17 pixel brightness data for a plurality of pixels, each of the

18 pixels having at least one color component and having a pixel

19 position; specifying the horizontal and vertical dimensions of a

20 bounding rectangle; determining an enlargement or reduction first

21 factor **f1** that, if applied, would resize the source image by

22 enlargement or reduction of its horizontal and vertical

23 dimensions so that the resized image is a largest replica of the

24 digitized image fitting entirely within the bounding rectangle;

25 forming an adjusted invisible image watermark that is enlarged of

26 reduced by a second factor **f2**; resizing the source image by

27 enlargement or reduction of its horizontal and vertical

28 dimensions by a combined common factor, **f1** times **f2**, to form an

29 alternative adjusted digital image. In some embodiments, the

30 method includes inserting the adjusted invisible image watermark

31 into the alternative adjusted digital image, and/or the factor **f2**

32 is greater than 0.1.

-13-

The present invention also includes a method for detecting a watermark imbedded in a candidate image employing a bounding rectangle, including the steps of: recalling dimensions of the bounding rectangle used to produce a resized source image from which the candidate image was produced; forming a resized image by resizing the horizontal and vertical dimensions of the candidate image by a common factor so the resized image is the largest replica of the candidate image fitting entirely within the bounding rectangle; reproducing the watermark suspected of being in the candidate image; and attempting detection of the watermark in the resized image. In some embodiments, the method further includes employing results obtained from the step of attempting, and/or determining if the candidate is a derivative copy of the source image.

Variations described for the present invention can be realized in any combination desirable for each particular application. Thus particular limitations, and/or embodiment enhancements described herein, which may have particular advantages to the particular application need not be used for all applications. Also, not all limitations need be implemented in methods, systems and/or apparatus including one or more concepts of the present invention. The invention also includes apparatus for implementing steps of method of this invention.

The present invention can be realized in hardware, software, or a combination of hardware and software. An image resizing tool and a watermark detection tool according to the present invention can be realized in a centralized fashion in one computer system, or in a distributed fashion where different elements are spread across several interconnected computer systems. Any kind of computer system - or other apparatus adapted for carrying out the

1 methods and/or functions described herein - is suitable. A

2 typical combination of hardware and software could be a general

3 purpose computer system with a computer program that, when being

4 loaded and executed, controls the computer system such that it

5 carries out the methods described herein. The present invention

6 can also be embedded in a computer program product, which

7 comprises all the features enabling the implementation of the

8 methods described herein, and which - when loaded in a computer

9 system - is able to carry out these methods.

10 Computer program means or computer program in the present context

11 include any expression, in any language, code or notation, of a

12 set of instructions intended to cause a system having an

13 information processing capability to perform a particular

14 function either directly or after conversion to another language,

15 code or notation, and/or reproduction in a different material

16 form.

17 Thus the invention includes an article of manufacture which

18 comprises a computer usable medium having computer readable

19 program code means embodied therein for causing a function

20 described above. The computer readable program code means in the

21 article of manufacture comprises computer readable program code

22 means for causing a computer to effect the steps of a method of

23 this invention. Similarly, the present invention may be

24 implemented as a computer program product comprising a computer

25 usable medium having computer readable program code means

26 embodied therein for causing a function described above. The

27 computer readable program code means in the computer program

28 product comprising computer readable program code means for

29 causing a computer to effect one or more functions of this

30 invention. Furthermore, the present invention may be implemented

31 as a program storage device readable by machine, tangibly

1 embodying a program of instructions executable by the machine to
2 perform method steps for causing one or more functions of this
3 invention.

4 It is noted that the foregoing has outlined some of the more
5 pertinent objects and embodiments of the present invention. This
6 invention may be used for many applications. Thus, although the
7 description is made for particular arrangements and methods, the
8 intent and concept of the invention is suitable and applicable to
9 other arrangements and applications. It will be clear to those
10 skilled in the art that modifications to the disclosed
11 embodiments can be effected without departing from the spirit and
12 scope of the invention. The described embodiments ought to be
13 construed to be merely illustrative of some of the more prominent
14 features and applications of the invention. Other beneficial
15 results can be realized by applying the disclosed invention in a
16 different manner or modifying the invention in ways known to
17 those familiar with the art.